

FY 2003 ITL Publications

Note that some documents are published in more than one place. Due to the large number of documents, publications listed in previous ITL Technical Accomplishment reports are not repeated.

Author	Title	Place of Publication
Beichl, I.	Dealing with Degeneracy in Triangulation	IEEE Computing in Science and Engineering 4, No. 6, November-December 2002, pp. 70-74

This is a tutorial article on a quick method for dealing with degeneracy in geometric computations with specific reference to triangulation. The type degeneracy targeted by this article that of four or more points on a circle and five or more points on a sphere.

Beichl, I., Sullivan, F.	Applications of Sinkhorn Balancing: The Monomer-Dimer Problem	Stochastic Processes and Functional Analyses, a volume in the series Lecture Notes in Pure & Applied Mathematics, Marcel Dekker, Publisher
--------------------------	---	--

We describe a general Monte Carlo technique based on work of Knuth for estimating the size of trees in backtrack algorithms. This method, based on importance sampling, is used to estimate the number of partial and complete matchings in a bipartite graph. Applications to the dimmer covering problem and the monomer-dimer problem are detailed.

Blackburn, D.M., Lazarick, R., Miles, C., Phillips, P.J., Podio, F.L.	2003 U.S. Government Biometrics Workshop: Overview and Summary	Web (http://www.biometricscatalog.org)
---	--	---

This document presents an overview and summary of the 2003 U.S. Government Biometrics Workshop, April 9, 2003.

Bowers, K., Mills, K., Rose, S.	Self-Adaptive Leasing for Jini	2003 IEEE International Conference on Pervasive Computing and Communications (PerCom)
---------------------------------	--------------------------------	---

Distributed computing environments require strategies by which components can detect and recover from failures in remote, collaborating components. Many protocols for distributed systems employ a strategy based on leases, which grant a leaseholder with access to data or services for a limited time (the lease period). If the leaseholder does not renew a lease before expiration of the lease period, the lease grantor assumes the leaseholder has failed and terminates the lease (withdrawing the previously granted access). Choosing an appropriate lease period requires consideration of tradeoffs among resource utilization, responsiveness, and the number of leaseholders. We investigate these issues in the context of Jini Network Technology, a service-discovery protocol created by Sun Microsystems. First, we establish quantitative tradeoffs among lease period, bandwidth utilization, responsiveness, and system size. Then, we consider two self-adaptive algorithms that enable a Jini

system, given a fixed allocation of resources, to vary lease periods to achieve the best responsiveness as system size varies. We compare the performance of these self-adaptive algorithms against each other, and against fixed lease periods chosen to accommodate a specific system size. We find that one of the self-adaptive algorithms, based on a simple restriction to the Jini specification, proves easy to implement and performs reasonably well. We anticipate that similar procedures could add self-adaptive capability to other distributed systems that rely on leases.

Bullen IV, H.W., Chang, J.S., Harn, A.V., Kelly, S.P., Satterfield, S.G., Ketcham, P.M., Devaney, J.E. A Glyph Toolbox for Immersive Scientific Visualization NISTIR 6924

We describe a set of software, The Glyph ToolBox (GTB), for creating three-dimensional (3D) glyphs. This software defines a single, general format for describing glyphs; it includes color and opacity parameters as well as location information. GTB is written with the UNIX philosophy of small reusable programs that are text based for portability and efficiency. Version 1.0 of GTB currently contains simple figures, manipulation functions, extrusion functions, meta-figure functions, as well as additional functions such as text creators. We describe four applications of the glyph toolbox: a visualization of the Monk's problem, a relationship highlighter, a smiley emoticon, and a display algorithm for concave surfaces. We separate the creation of the glyphs from their display. We provide a filter that can translate the GTB format to Inventor format or VRML 1.0. However, any system can incorporate the GTB format into their environment, making the creation and use of glyphs uniform across viewers.

Burr, W.E. The Advanced Encryption Standard (AES): Raising the Bar for Cryptography IEEE Security and Privacy

This paper describes how the National Institute of Standards and Technology (NIST) selected the Advanced Encryption Standard (AES), a new standard symmetric key encryption algorithm that has been adopted for use by the U.S. Federal Government, for Standards and Technology (NIST). The paper also describes the NIST follow-on efforts to bring other federal cryptographic standards up to the same level of strength as AES and to update and extend the NIST standard cryptographic modes of operation.

Byers, F.R. Care and Handling of CDs & DVDs -- A Guide for Librarians and Archivists NIST SP and Council on Library Information Resources Report

This document is a comprehensive review of procedures for the care and handling of optical disc media, providing both guidelines and introductory information for both the expert and the end user (librarians, archivists) of CDs and DVDs.

Casasent, D., Watson, C. Correlation Filters for Elastic-Distorted Live-Scan Fingerprint Recognition NISTIR

This is a summary of a multi-year study of the use of distortion-invariant filters for recognition of live-scan dab fingerprints with elastic distortions. These fingerprints are characterized by elastic distortions. NIST special database 24 is used; it represents the only available database containing a number of elastic distortions for each fingerprint. Several different distortion-invariant filters were addressed including two new ones that used high-pass filtered fingerprint data to improve discrimination. Verification and identification applications are addressed and test procedures for evaluating algorithms/systems for each are defined.

Chandramouli, R.

Specification and Validation of
Enterprise Access Control Data for
Conformance to Model and Policy

7th World Multiconference on
Systemics, Cybernetics and
Informatics (SCI 2003) ,Orlando,
Florida, July 27-30, 2003

The effectiveness of an enterprise access control framework depends upon the integrity of the various components or the building blocks used in that framework. The essential components of that framework are: (a) an Enterprise Access Control Model (b) a Validation mechanism to verify the enterprise access control data developed based on that model, for conformance to the model as well as domain-specific policy constraints and (c) a mechanism to map the enterprise access control data into formats required by native access enforcement mechanisms in the heterogeneous application systems in the enterprise. In this paper we chose the Role-based Access Control Model (RBAC) as a candidate for the enterprise access control model. We develop an XML Schema of an RBAC Model for a specific enterprise context and demonstrate the use of schema features to specify structural and some rudimentary domain constraints. We then annotate that XML Schema of an Enterprise RBAC Model to demonstrate specification and enforcement of some important domain-specific policy constraint using the Schematron language.

Coakley, K.J., Downing, R.G.,
Lamaze, G. P., Hofsass, H. C.,
Ronning, C., Biegel, J.

Erratum: Modeling Detector Response
for Neutron Depth Profiling

Nuclear Instruments and Methods in
Physics Research A

In a previous paper, we analyzed the Neutron Depth Profiling energy spectrum collected from a diamond-like carbon (DLC) sample doped with boron. Based on a numerical model for the Detector Response Function (DRF), we estimated a theoretical boron profile consisting of four plateaus by a nonlinear regression method. In our approach, we predicted the observed NDP spectrum based on the estimated boron profile and the DRF which depends on energy broadening due to straggling, multiple scattering and the energy resolution of the detector. To get good agreement between the observed and predicted NDP spectrum, we inflated the energy broadening due to straggling. However, we underestimated the contribution of multiple scattering for the DLC sample due to a computational error. When the predicted energy broadening due to multiple scattering is properly computed, the observed and predicted NDP spectrum agree well without inflating the energy broadening due to straggling. The new estimate of the boron profile, determined by fitting a four plateau model to the observed NDP spectrum, is in reasonably good agreement with the theoretical boron profile.

Coakley, K.J., McKinsey, D.N.

Spatial Methods for Event
Reconstruction in CLEAN

Nuclear Instruments and Methods in
Physics Research A

In CLEAN (Cryogenic Low Energy Astrophysics with Noble gases), a proposed neutrino and dark matter detector, background discrimination is possible if one can determine the location of an event with high accuracy. Here, we develop spatial methods for event reconstruction, and study their performance in computer experiments. We simulate ionizing radiation events that produce multiple scintillation photons within a spherical detection volume filled with liquid neon. We estimate the radial location of a particular ionizing radiation event based on the observed count data corresponding to that event. The count data is collected by detectors mounted at the spherical boundary of the detection volume. We neglect absorption, but account for Rayleigh scattering. To account for wavelength shifting of the scintillation light, we assume that photons are absorbed and re-emitted at the detectors. In our study, the detectors incompletely cover the surface area of the sphere. In one method, we estimate the radial location of the event by maximizing the approximate Poisson likelihood of the observed count data. To correct for

scattering and wavelength-shifting, we adjust this estimate using a polynomial calibration model. In the second method, we predict the radial location of the event as a polynomial function of the magnitude of the Centroid of the observed count data. The polynomial calibration models are constructed from calibration (training) data. In general, the Maximum Likelihood method estimate is more accurate than the centroid method estimate. We estimate the expected number of photons emitted by the event by a Maximum Likelihood method and a simple method based on the ratio of the number of detected photons and a detection probability.

Dabrowski, C.E., Mills, K.L.

Understanding Self-Healing in
Service-Discovery Systems

Workshop on Self-Healing Systems
(WOSS'02)

Service-discovery systems aim to provide consistent views of distributed components under varying network conditions. To achieve this aim, designers rely upon a variety of self-healing strategies, including: architecture and topology, failure-detection and recovery techniques, and consistency maintenance mechanisms. In previous work, we showed that various combinations of self-healing strategies lead to significant differences in the ability of service-discovery systems to maintain consistency during increasing network failure. Here, we ask whether the contribution of individual self-healing strategies can be quantified. We give results that quantify the effectiveness of selected combinations of architecture-topology and recovery techniques. Our results suggest that it should prove feasible to quantify the ability of individual self-healing strategies to overcome various failures. A full understanding of the interactions among self-healing strategies would provide designers of distributed systems with the knowledge necessary to build the most effective self-healing systems with minimum overhead.

Dabrowski, C.E., Mills, K.L.,
Rukhin, A.L.

Performance of Service-Discovery
Architectures in Response to Node
Failures

2003 International Conference on
Software Engineering and Practice
(SERP'03), Las Vegas, Nevada,
June 23-26, 2003

Current trends suggest future software systems will rely on service-discovery protocols to combine and recombine distributed services dynamically in reaction to changing conditions. We investigate the ability of selected designs for service-discovery protocols to support real-time distributed control applications by detecting and recovering from failure of remote services. We model two architectures (two-party and three-party) underlying most commercial service-discovery systems. We use simulation to quantify functional effectiveness achieved by the two architectures as the rate of failure increases for remote services. We further decompose non-functional periods into failure-detection delay and restoration delay. Our quantitative measurements suggest that a two-party architecture yields better robustness than a three-party architecture. We discuss the underlying causes of this outcome.

Dray, J.

NIST Publishes Smart Card
Interoperability Specifications

NIST Journal of Research

This summary is extracted from the July 2002 ITL Bulletin summarizes the Government Smart Card Interoperability Specification, which provides solutions to a number of the interoperability problems associated with smart card technology.

Fabijonas, B.R., Lozier, D.W.,

Algorithms and Codes for the

NISTIR 6596 and Journal of

Godil, A., Grother, P., Ressler, S.

Human Identification from Body Shape

The Fourth International Conference
on 3D Digital Imaging and
Modeling, Alberta, Canada

In this paper, we investigate the utility of static anthropometric distances as a biometric for human identification. The 3D landmark data from the CAESAR database is used to form a simple biometric consisting of distances between fixed rigidly connected body locations. This biometric is overt, and invariant to view and body posture. We use this to quantify the asymmetry of human bodies, and to characterize the interpersonal and intrapersonal distance distributions. The former is computed directly and the latter by adding zero-mean gaussian noise to the landmark points. This simulation framework is applicable to arbitrary shape based biometric. We use gross body proportions information to model a computer vision recognition system.

Golmie, N.

Bluetooth Dynamic Scheduling and
Interference Mitigation

ACM/Kluwer Journal on Special
Topics in Mobile Networking and
Applications (MONET) in 2003,
issue of Advances in Research of
Wireless Personal Area Networking
and Bluetooth Enabled Networks

Bluetooth is a cable replacement technology for Wireless Personal Area Networks. It is designed to support a wide variety of applications such as voice, streamed audio and video, web browsing, printing, and file sharing, each imposing a number of quality of service constraints including packet loss, latency, delay variation, and throughput. In addition to QoS support, another challenge for Bluetooth stems from having to share the 2.4 GHz ISM band with other wireless devices such as IEEE 802.11. The main goal of this paper is to investigate the use of a dynamic scheduling algorithm that guarantees QoS while reducing the impact of interference. We propose a mapping between some common QoS parameters such as latency and bit rate and the parameters used in the algorithm. We study the algorithm's performance and obtain simulation results for selected scenarios and configurations of interest.

Golmie, N., Rebala, O.

Techniques to Improve the
Performance of TCP in a Mixed
Bluetooth and WLAN Environment

Proceedings of the IEEE
International Conference on
Communications (ICC 2003),
Anchorage, Alaska, May 11-15, 2003

A major challenge for the WLAN technology stems from having to share the 2.4 GHz ISM band with other wireless devices such as Bluetooth radios. The main goal of this paper is to investigate the use of techniques to mitigate the effects of interference for Bluetooth and WLAN and discuss the resulting performance trade-offs. We compare the performance of the Bluetooth and WLAN systems and evaluate how each technique improves or degrades the TCP performance. Simulation results for selected scenarios and configurations of interest are obtained and the performance of Bluetooth and WLAN is measured in terms of packet loss, TCP throughput and delay.

Griffith, D.W., Lee, S.

Dynamic Expansion of M:N Protection

Proceedings of the 2002

In order to provide reliable connections across metropolitan and wide-area optical networks, the network operator must provide some degree of redundancy so that traffic can be switched from damaged working paths to backup paths that are disjoint from the working paths that they are protecting. In the most general form of path protection, N working paths between two client edge nodes are protected by M backup paths. The set of working and protection paths forms a $M:N$ protection group. In the near future, optical transport networks (OTNs) will use an automated control plane to set up, tear down, or modify connections between client edge nodes. If protection groups are allowed to evolve over time, with working and backup paths being set up or torn down individually, it may be necessary to modify other working and backup paths in addition to those that are being created or destroyed, in order to maximize network utilization. In this paper, we examine the mechanisms that can support adaptive $M:N$ protection group management and describe how existing Generalized Multi-Protocol Label Switching (GMPLS) signaling protocols allow this capability to be deployed in the OTN.

Griffith, D.W., Lee, S., Krivulina, L.

The Effect of Delay Mismatch in MPLS
Networks Using 1+1 ProtectionProceedings of the 2002
International Conference on Parallel
Processing, Vancouver, Canada,
August 18-21, 2002

High-capacity optical-fiber backbone networks protect information flows belonging to their premium customers by routing two copies of the customer's data over disjoint paths. This scheme, known as 1+1 protection, ensures that the customer will experience no service interruptions even if a fiber cut occurs somewhere in the network. A protection scheme based on this concept was proposed for Multi-Protocol Label Switched (MPLS) packet flows at the Spring, 2002, meeting of the Internet Engineering Task Force (IETF) by a team from Lucent. The Lucent proposal will require the MPLS routers located at the ingress and egress edges of the MPLS network to protect certain data flows by creating two disjoint label switched paths (LSPs). Packets using the 1+1 protection service are duplicated at the ingress router, assigned an ID number, and sent to the egress router over the two LSPs. The egress router retrieves the least-delayed copy of each packet and forwards it to the destination, discarding the more-delayed copy. A sliding window allows the egress router to function even when packet losses occur. This scheme allows data to flow even if a link failure occurs on one of the LSPs, but a sufficiently large difference in the propagation delays associated with the two protection LSPs can cause performance degradations that may reduce the protected flow's quality of service (QoS) below what is acceptable to the customer. In this paper we examine the impact of delay mismatch on the probability of packet loss and on packet jitter, and we show that both of these metrics are adversely affected by large LSP delay differences.

Grother, P., Micheals, R.J., Phillips,
P.J.Face Recognition Vendor Test 2002
Performance Metrics

NISTIR 6982 and AVBPA 2003

We present the methodology and recognition performance characteristics used in the Face Recognition Vendor Test 2002. We refine the notion of a biometric imposter, and show that the traditional measures of identification and verification performance are limiting case specializations of a novel watch list scenario. The watch list problem is a newly important and operationally

realistic generalization of both detection and identification of persons of interest, together with simultaneous verification-like constraints on false alarm rates. In addition, we use performance scores on disjoint populations to establish a novel means of computing and displaying distribution-free estimates of the variation of verification vs. false alarm performance. Finally, we formalize gallery normalization, which is an extension of previous evaluation methodologies; we define a pair of gallery dependent mappings that can be applied as a post recognition step to vectors of distance or similarity scores. All the methods are biometric non-specific, and applicable to large populations.

Gurski, K.F., Kollar, R., Pego, R.L. Slow Damping of Internal Waves in a Proceedings of the Royal Society
Stably Stratified Fluid of London

We study the damping of internal gravity waves in a stably stratified fluid with constant viscosity in two- and three-dimensional bounded domains. For the linearized Navier-Stokes equations for incompressible flow with no-slip boundary conditions that model this fluid, we prove there are non-oscillatory normal modes with arbitrarily small exponential decay rates. The proof is very different from that for a horizontally periodic layer and depends on a structure theorem for compact operators which are self-adjoint with respect to an indefinite scalar product in a Hilbert space. We give a complete proof of this theorem, which is which is closely related to results of Pontrjagin.

Hagedorn, J.G., Martys, N.S., Breakup of a Fluid Thread in a Confined Physical Review E
Douglas, J.F. Geometry: Droplet-Plug Transition
Perturbation Sensitivity and Kinetic
Stabilization With Confinement

We investigate the influence of geometrical confinement on the breakup of long fluid threads in the absence of imposed flow using a Lattice Boltzmann model. Our simulations primarily focus on the case of threads centered coaxially in a tube filled with another Newtonian fluid and subjected to both impulsive and random perturbations. We observe a 'glass-like' slowing down of the rate of thread breakup ('kinetic stabilization') over a wide range of the confinement, $2.5 \leq \text{equivalent conductivity} (= R^2_{\text{tube}}/R^2_{\text{thread}}) \leq 10$ and find that the relative surface energies of the liquid components influence this effect. For equivalent conductivity < 2.3 , there is a transition in the late-stage morphology between spherical droplets and tube 'plugs'. Unstable distorted droplets ('capsules') form as transient structures for intermediate confinement (equivalent conductivity ≈ 2.1). The thread breakup process for more highly confined threads (equivalent conductivity ≤ 1.9) is sensitive to the nature of the initial thread perturbation. Impulsive perturbations led to a 'bulging' of the fluid near the tube wall, followed by thread breakup through the propagation of wave-like disturbances ('end-pinch instability') initiating from thread rupture points that 'nucleate' from the thread bulges. Random impulses along the thread modeling thermal fluctuations, led to a complex breakup process involving a competition between the capillary wave and end-pinch instabilities. We also briefly compare our simulations to threads confined between parallel plates and to multiple interacting threads under confinement.

Harman, D.K. The Development and Evolution of Proceedings of the Third NTCIR
TREC and DUC Workshop on Research in
Information Retrieval, Automatic
Text Summarization and Question

Answering (Sept. 2001 – Oct. 2002)

The Text REtrieval Conference (TREC) has been running for 11 years now, with 93 participants in the last round of evaluation. This paper chronicles the changes in TREC over that time, emphasizing the evolution in the tasks that were evaluated rather than discussing the results of the specific evaluations. The development of the new Document Understanding Conference (DUC) is also discussed, including the evaluation issues that have surfaced during its first two years.

Harman, D.K. Overview of the TREC 2002 Novelty Included in NIST SP 500-251, The Eleventh Text Retrieval Conference (TREC 2002)

The novelty track was a new track in TREC-11. The basic task was as follows: given a TREC topic and an ordered list of relevant documents (ordered by relevance ranking), find the relevant and "novel" sentences that should be returned to the user from this set. There were 13 groups that participated in this new task.

Hash, J.S. NIST Information Security Standards Handbook on Audit and Control Standards, Best Practices and Guidelines for Information Security, Leon Strous, Editorin Chief, Kluwer International, Publisher

The submission is a chapter describing NIST security standards (FIPS and Special Publication series 800). The author's instructions were that NIST prepare chapter summarizing standards indicating title, dates, publications, and brief summaries.

He, S.X., Yang, G.L., Fang, K.T., Consistent Estimation of Poisson Journal of the American Statistical Widmann, J.F. Intensity in the Presence of Dead Time Association

Phase Doppler Interferometry (PDI) is a non-intrusive technique frequently used to obtain information about spray characteristics. Understanding spray characteristics is of critical importance in many areas of science, including liquid fuel spray combustion, spray coatings, fire suppression, and pesticides. PDI measures the size and velocity of individual droplets in the spray. Due to the design of the instrument, the recordings of the PDI contain gaps, called dead times. The presence of the recurrent dead times greatly complicates the estimation of the diffusion rate of the droplets. Modeling the spray process as a homogeneous Poisson process, we construct consistent estimators of the diffusion rate (Poisson intensity) under various conditions. Asymptotic normality of the estimators are discussed. Simulation results indicate good agreement of our estimators (in the presence of dead time) with the MLE obtained without dead time. For illustration, experimental data are used to estimate the Poisson intensity.

Heckert, N.A., Filliben, J.J., Handbook 151: NIST/SEMATECH Web Croarkin, M.C., Hembree, B., e-Handbook of Statistical Methods (<http://www.itl.nist.gov/div898/handbook/>) Guthrie, W.F., Tobias, P., Prinz, J.

The URL is <http://www.itl.nist.gov/div898/handbook/mpc/mpc.htm>. This is a web-based guide to statistical methods for engineering. It involves case studies with interactive software for analysis.

Hogan, M.D. "Are you who you claim to be?" ISO Bulletin, Vol. 34, No. 3, March 2003

Key Comparisons Studies

Results of International Key Comparisons of National Measurement Standards provide the technical basis for the Mutual Recognition Arrangement formulated by Le Comite International des Poids et Mesures. With many key comparisons already completed and a number of new key comparison experiments currently under way, we now have a better understanding of the statistical issues that need to be addressed for successfully analyzing key comparisons data and making proper interpretations of the results. There is clearly a need for a systematic approach for statistical analyses of key comparisons data that can be routinely implemented by all participating laboratories. In this paper we review a number of questions that arise in the context of statistical modeling and analysis of international key comparisons data and propose a systematic approach for answering these questions. The proposed approach is illustrated using real data from key comparison experiments.

Jansen, W.A.

Authenticating Users on Handheld

Canadian Information Technology
Security Symposium, May 12-15, 2003

Adequate user authentication is a persistent problem, particularly with handheld devices, which tend to be highly personal and at the fringes of an organization's influence. Yet, these devices are being used increasingly in corporate settings where they pose a security risk, not only by the sensitive information they may contain, but also the means to access such information they may provide. User authentication is the first line of defense against a lost or stolen device. Motivating users to employ common password mechanisms and periodically change their authentication information to meet corporate policy is always a challenge, and particularly so for handheld devices. This paper reviews alternative mechanisms, which are compatible with the capabilities of handheld devices and designed to facilitate user authentication, to replace passwords.

Jansen, W.A., Karygiannis, T.,
Korolev, V., Gavril, S., Iorga, M.

Policy Expression and Enforcement for
Handheld Devices

First International Conference on
Security in Pervasive Computing

The use of mobile handheld devices, such as Personal Digital Assistants (PDAs) and tablet computers, within the workplace is expanding rapidly. These devices are no longer viewed as coveted gadgets for early technology adopters, but instead have become indispensable tools that offer competitive business advantages for the mobile workforce. While providing productivity benefits, the ability of these devices to store and transmit corporate information through both wired and wireless networks poses potential risks to an organization's security. This paper describes a framework for managing user privileges on handheld devices. The approach is aimed at assisting enterprise security officers in administering and enforcing group and individual security policies for PDAs, and helping constrain users to comply automatically with their organization's security policy. Details of a proof-of-concept implementation of the framework are also provided.

Jansen, W.A., Korolev, V.

Picture Password: A Visual Login
Technique for Linux PDAs

Annual Computer Security
Applications Conference, December
8-12, 2003

Adequate user authentication is a persistent problem, particularly with handheld devices, which tend to be highly personal and at the fringes of an organization's influence. Yet, these devices are being used increasingly in corporate settings where they pose a security risk, not only by containing sensitive information, but also by providing the means to access such information over wireless network interfaces. User authentication is the first line of defense against a lost or stolen PDA. However, motivating

users to enable simple PIN or password mechanisms and periodically update their authentication information is a constant struggle. This paper describes a means to authenticate a user to a PDA using a visual login technique called Picture Password. The underlying rationale is that a method for login based on visual image selection is an easy and natural way for users to authenticate, removing the most serious barriers to users' compliance with corporate policy. While the technique was designed specifically for handheld devices, it is also suitable for notebooks, workstations, and other computational devices.

Kacker, R., Jones, A. On Use of Bayesian Statistics to Make Metrologia
Guide to the Expression of Uncertainty
in Measurement Consistent

The Guide to the expression of uncertainty in measurement recommends a standardized way of expressing uncertainty in measurement and provides a comprehensive approach for combining information to evaluate uncertainty in all kinds of measurements in science, engineering, commerce, industry, and regulation. The Guide is being increasingly recognized from national metrology institutes to industrial laboratories. However the Guide is not fully consistent, which may impede its influence. The Guide supports uncertainties evaluated from statistical methods, referred to as Type A, and those determined by other means, referred to as Type B. The Guide recommends classical (frequentist) statistics for evaluating the Type A components of uncertainty but it interprets the combined uncertainty from Bayesian viewpoint. We suggest that the Guide can be made consistent by requiring that all Type A uncertainties be evaluated from Bayesian statistics or interpreted as their approximations. In applications of interest to metrologists, the Type A uncertainties evaluated from classical statistics may be used as approximations provided they are interpreted from Bayesian viewpoint.

Karygiannis, T., Owens, L. Wireless Security - 802.11, Bluetooth™ NIST SP 800-48
and Handheld Devices (http://csrc.nist.gov/publications/nist_pubs/index.html)

The purpose of this document is to provide agencies with guidance for establishing secure wireless networks. Agencies are encouraged to tailor the recommended guidelines and solutions to meet their specific security or business requirements. However, NIST recommendations are not intended to supersede an agency's existing security policy. The document addresses two wireless technologies that government agencies are most likely to employ: wireless local area networks (WLAN) and ad hoc or, more specifically, Bluetooth networks. The document also addresses the use of wireless handheld devices. The document does not address technologies such as wireless radio and other WLAN standards that are not designed to the Institute of Electrical and Electronics Engineers (IEEE) 802.11 standard. These technologies are considered out of the scope of this document.

Kearsley, A.J. A Matrix-Free Algorithm for the SIAM Journal on Optimization
Large-Scale Constrained Trust-Region
Subproblem

A new "matrix-free" algorithm for the solution of linear inequality constrained, large-scale trust-region sub-problems is presented. The matrix-free nature of the algorithm eliminates the need for any matrix factorizations and only requires inner products between vectors and rows/columns of matrices. Numerical results that demonstrate the viability of the approach are included.

Kearsley, A.J., Wallace, W.E.,
Guttman, C.M. A Numerical Method for Mass Spectral
Data Analysis Applied Mathematics Letters

The new generation of mass spectrometers produces an astonishing amount of high-quality data in a brief period of time leading to inevitable data analysis bottlenecks. Automated data analysis algorithms are required for rapid and repeatable processing of mass spectra containing hundreds of peaks, the part of the spectra containing information. New algorithms must work with minimal user input, both to save operator time and to eliminate inevitable operator bias. Toward this end an accurate mathematical algorithm is presented that automatically locates and calculates the area beneath peaks. Promising numerical

Kuhn, D.R. Vulnerabilities in Quantum Key
Distribution Protocols NISTIR 6977

Recently proposed quantum key distribution protocols are shown to be vulnerable to a classic man-in-the-middle attack using entangled pairs created by Eve. The attack could be applied to any protocol that relies on manipulation and return of entangled qubits to create a shared key. The protocols that are cryptanalyzed in this paper were proven secure with respect to some eavesdropping approaches, and results reported here do not invalidate these proofs. Rather, they suggest that quantum cryptographic protocols, like conventional protocols, may be vulnerable to methods of attack that were not envisaged by their designers.

Kuhn, D.R., Chandramouli, R.,
Butler, R.W. Cost Effective Use of Formal Methods
in Verification and Validation Foundations 02 V&V Workshop,
Laurel, Maryland, October 22-23, 2002

Formal methods offer the promise of significant improvements in verification and validation, and may be the only approach capable of demonstrating the absence of undesirable system behavior. But it is widely recognized that these methods are expensive, and their use has been limited largely to high-risk areas such as security and safety. This paper focuses on cost-effective applications of formal techniques in V&V, particularly recent developments such as automatic test generation and use of formal methods for analyzing requirements and conceptual models without a full-blown formal verification. We also discuss experience with requiring the use of formal techniques in standards for commercial software.

Lee, S., Griffith, D.W., Song, N-O. An Analytical Approach to Shared
Backup Path Provisioning in GMPLS Proceedings of the Military
Communications Conference
(MILCOM 2002), Anaheim, California

As GMPLS and its supporting set of protocols develop into a viable control plane for optical networks, an important function that they will need to support will be the restoration and protection function that has been a major feature of legacy optical networks. Several models have been proposed for protection with GMPLS using shared backup paths. This previous work has not investigated the effect on recovery time (i.e., service interruption time) critical to the service or the number of backup paths that are required to meet a desired level of performance. Using both recovery time and recovery failure probability, we have developed a new analytic model for GMPLS-based recovery in M:N protection groups.

Lee, S., Kim, C., Griffith, D.W. Hierarchical Restoration Scheme for
Multiple Failures in GMPLS Networks Proceedings of the 2003
International Conference on
Communications, Anchorage, Alaska,

May 11-15, 2003

It is expected that GMPLS-based recovery could become a viable option for obtaining faster restoration than layer 3 rerouting. Even though dedicated restoration ensures restorability of connections, exclusive use of dedicated scheme would result in wasting network resources, especially in case of providing for multiple failures. A range of restoration schemes has been proposed that use the concept of sharing capacity to improve efficiency. However, the case of multiple simultaneous failures has not been considered. In this paper we propose a hierarchical scheme for handling multiple simultaneous failures, where hierarchical Shared Risk Link Groups (SRLGs) are applied. We also introduce Backup Group Multiplexing (BGM) into our hierarchical scheme to precipitate the restoration of multiple Label Switched Paths (LSPs) with failures all at once. Furthermore, the proposed scheme selects a backup path with enough resources to satisfy renegotiated Quality of Service (QoS) of each backup group, among M backup paths. Our simulation results demonstrate that our scheme utilizes bandwidth more efficiently through multiplexing gain.

Lennon, E.B., Editor

Security Patches and the CVE
Vulnerability Naming Scheme: Tools to
Address Computer System

ITL Bulletin, October 2002

Today more than ever, timely response to vulnerabilities is critical to maintain the operational availability, confidentiality, and integrity of information technology (IT) systems. To assist federal agencies and industry respond to vulnerabilities in a timely manner, ITL recently released two new publications dealing with vulnerabilities in computer systems: NIST Special Publication (SP) 800-40, Procedures for Handling Security Patches, by Peter Mell and Miles C. Tracy, and NIST SP 800-51, Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme, by Peter Mell and Tim Grance. This ITL Bulletin summarizes these two documents on system vulnerabilities, available at <http://csrc.nist.gov/publications/nistpubs/index.html>.

Lennon, E.B., Hawes, K.

2002 ITL Technical Accomplishments

NISTIR 6909

This report presents the achievements and highlights of NIST's Information Technology Laboratory during FY 2002. Following the Director's Foreword and the ITL overview, technical projects in ITL focus areas are described, followed by services to NIST, industry and international interactions, and staff recognition.

Liggett, W.S.

Parameter Design for Measurement
Protocols by Latent Variable Methods

Technometrics

We present an approach to measurement system parameter design that does not require the values of the experimental units be known. The approach does require experimental units grouped in classes, a necessity when protocol execution alters the unit. A consequence of these classes is that the approach admits replication. This paper presents maximum likelihood estimates with a comparison to similar estimates in factor analysis, strategies for noise factors including those connected with secondary properties of the experimental units, and Bayesian inference on experimental contrasts through Markov chain Monte Carlo. The approach is illustrated by solderability measurements made with a wetting balance.

Liu, H., Zhang, N.F.

Performance Evaluation of Approaches
to Combining Results From Multiple

Proceedings of the 2002 Joint
Statistical Meetings

The problem of determining a consensus mean and its uncertainty from the results of multiple measurement methods or

laboratories is an important problem. Many solutions, both Bayesian and non-Bayesian, to this problem have been proposed over the years, including those developed by NIST. However, objective performance comparisons of the proposed solutions have not been studied. In this paper, we will examine desirable criteria for comparison, and use them to compare the existing solutions.

Lu, Z.Q.J., Sedransk, N.

Generalized Pareto Mixture Distribution
Approach to Network Modeling and
Performance Evaluation 1

IEEE Transactions on Signal
Processing

A recurring theme in Internet network traffic analysis is that most observed data show characteristics of a long (heavy) right-tail distribution taking on nonnegative values. Thus, extreme value distribution such as generalized Pareto distribution (GPD) provides a natural setup for modeling the tail behavior of network data. On the other hand, due to the enormous diversity in network traffic at different time scales, at different nodes, different sources or protocols, it is necessary to introduce a more flexible framework using finite mixtures. We believe that the generalized Pareto mixture distribution (GPMD) is such a general model and it should form a theoretical basis for any anomaly detection algorithms for extreme events detection. We will demonstrate these points through applying to the popular RTT pingER data. For example, in terms of pingER RTT performance, users might have felt more frequent network slowdowns even if the median performance improved after a NIST network upgrade. Potential extensions to include temporal dependence and continuous time process are also discussed. Our GPMD methodology as a powerful tool for detecting perturbations at extreme events may prove useful in other areas of network security.

Lyon, G.E.

A Quick-Reference List of
Organizations and Standards for Digital
Rights Management

NIST SP 500-241
(<http://www.itl.nist.gov/div895/docs/NIST241assm.9oct.pdf>)

The field of digital rights management (DRM) --also called intellectual property management and protection (IPMP)-- is today a swirling mix of technology, policy, law and business practice. There are many organizations active in the field. Under such circumstances, even a modest guide or index of active organizations can be useful. In March 2002, experts at a NIST cross-industry DRM workshop recommended that NIST take steps toward such a guide. With the help of numerous workshop participants and others, this is the first edition of a DRM quick-reference list.

Lyons-Burke, K.L.

Using the Computer Security Expert
Assist Team (CSEAT) Methodology to
Improve IT Security

Thirty-Sixth Hawaii International
Conference on System Sciences
(HICSS-36), January 6, 2003

CSEAT provides an independent review of an organization's IT security program. The CSEAT review is not an audit or an inspection. The CSEAT review is an assessment of the state of the organization's IT security maturity and the IT security policies, procedures, and security controls implementation and integration across all business areas. The CSEAT review provides a consistent and comparable approach to IT security through consistent application of security control objectives and IT security effectiveness criteria. CSEAT performs a comparable review of the organization's structure, culture, and business

mission. CSEAT utilizes extensive criteria containing specific control objectives against which an unclassified system or group of interconnected systems can be tested and measured. CSEAT has developed and maintains a computerized toolset to support the reviews. NIST's CSEAT does not establish new security requirements. The CSEAT security control objectives are abstracted directly from long-standing requirements found in federal government regulations, statutes, policies, and guidance on IT security. NIST IT security statutory responsibilities include: developing technical, management, physical, and administrative cost effective standards and guidance for IT security of Federal computer systems; and developing validation procedures for evaluating the effectiveness of standards and guidelines. The CSEAT review is based upon five stages of maturity: policy, procedures, implementation, test, and integration. Following the review, a prioritized action plan that can be implemented to improve agency or program IT security is provided to the organization.

Marbukh, V.

On Shortest Random Walks under
Adversarial Uncertainty

Proceedings of the 40th Allerton
Conference on Communications,
Control, & Computing, Champaign,
Illinois

Finding shortest feasible paths in a weighted graph has numerous applications including admission and routing in communication networks. This paper discusses a game theoretic framework intended to incorporate a concept of path stability into the process of shortest path selection. Route stability is an important issue in a wire-line and especially in wireless network due to node mobility as well as limited node reliability and power supply. The framework assumes that the link weights are selected within certain "confidence intervals" by an adversary or set of adversaries. The width of the confidence interval for the path weight represents the path stability. One of the immediate benefits of this framework is justification for randomized routing interpreted as a mixed Nash equilibrium strategy in the corresponding game. To demonstrate a wide range of possible applications of the proposed framework the paper briefly discusses possible application to robust traffic engineering.

Marbukh, V.

Network Provisioning as a Game
Against Nature

Proceedings of the IEEE
International Conference on
Communications (ICC 2003),
Anchorage, Alaska, May 11-15, 2003

Traditional approaches to network provisioning assume availability of the reliable estimates for the expected demands. This assumption, however, oversimplifies many practical situations when some incomplete information on the expected demands is available, and proper utilization of this information may improve the network performance. In a case of traffic engineering the uncertainty in the expected demands may be a result of sudden changes in the demand pattern, when significant statistical uncertainty in determining the varying demand pattern and possible undesirable transient effects make continuous adjustment of the routing algorithm to varying demands difficult. A long-term network provisioning, e.g., capacity planning, is a subject to uncertainties in the overall economic conditions. Despite the network may be capable of controlling demands through pricing, the overall economic conditions affect the price-demand curve. As the recent sharp downturn in the demand for communication bandwidth demonstrated, making long-term network planning decisions without assessing reliability of the underlying assumptions on the expected demands may lead to disastrous results. Assuming that the expected demand is an unknown mixture of some known scenarios, i.e., demand matrices, this paper proposes a framework for robust network provisioning by guarding against the worst case scenario with respect to the future demands. This framework can be interpreted as a game between the network, e.g., service provider, and nature. The service

provider makes the network provisioning decisions in an attempt to minimize losses due to the uncertain future demands, while the nature selects a feasible demand matrix. Solution to this game balances risks of over and under provisioning of the network.

Marbukh, V.

A Cognitive Framework for
Performance/Resilience Optimized
Multipath Routing in Networks with
Unstable Topologies

Proceedings of the IEEE Wireless
Communications and Networking
Conference (WCNC 2003), New
Orleans, Louisiana, March 16-20, 2003

This paper proposes a framework for optimized multipath routing in a wireless network with frequently changing topology. The topology changes may be due to node mobility in mobile ad hoc networks, or limited node reliability and power supply in sensor networks. The framework attempts to minimize losses (regrets) resulted from uncertainty in the network state at the point of making the routing decision. This uncertainty results from delays in propagating rapidly changing network state information and high cost of network state updates in terms of the network resources. The framework yields the optimal route mixture in the neighborhood of the “best” route. This is consistent with observation [1] that while a desirable goal is to deliver data along the best available (primary) route, maintaining multiple routes through multipath may have beneficial effect on the network performance due to keeping track of the “best” route. The proposed framework explicitly accounts for this effect by assuming that the routing affects the level of uncertainty. Resiliency of the routing under uncertainty may be achieved by assuming that the uncertainty is adversarial, given the available information on the network state. This framework naturally allows for the game theoretic interpretation with routing algorithm making a feasible routing decision and adversarial environment selecting a feasible, i.e., consistent with available information, network state. The optimal route mixture is identified with (generally mixed) Nash routing strategy in the corresponding game. Future efforts should be directed towards solving the corresponding games.

Martin, A.F., Przybocki, M.A.

NIST 2003 Language Recognition
Evaluation

Proceedings of Eurospeech '03,
Geneva, Switzerland, September 2003

The 2003 NIST Language Recognition Evaluation was very similar to the last such NIST evaluation in 1996. It was intended to establish a new baseline of current performance capability for language recognition of conversational telephone speech and to lay the groundwork for further research efforts in the field. The primary evaluation data consisted of excerpts from conversations in twelve languages from the CallFriend Corpus. These test segments had durations of approximately three, ten, or thirty seconds. Six sites from three continents participated in the evaluation. The best performance results were significantly improved from those of the previous evaluation.

McCabe, R.M.

Fingerprint Interoperability Standards

Advances in Fingerprint Recognition
(Publisher: Springer)

The commercialization of the Automatic Fingerprint Identification System (AFIS) began in the mid 1970's with the installation of five systems at the FBI. In subsequent years, additional vendors developed competing AFISs without considering any aspects of fingerprint data exchange between the systems. This chapter will describe and review the standards created to effect interoperability between dissimilar systems, the certification procedure for the WSQ compression algorithm, image quality issues, and the reference databases developed to assist manufacturers and researchers.

McLarnon, M., Swanson, M., Editor Automated Security Self-Evaluation NISTIR 6951
Tool Technical Documentation

The Automated Security Self-Evaluation Tool (ASSET) automates the process of completing a system self-assessment. ASSET will assist organizations in completing the self-assessment questionnaire contained in NIST Special Publication (Special Publication) 800-26, Security Self-Assessment Guide for Information Technology Systems. This technical manual is intended as a development guide for software engineers/database administrators who wish to troubleshoot unique installations of ASSET, reproduce the development version of ASSET, or extend the functionality of ASSET.

Mell, P., Lippmann, R., Hu, V., An Overview of Issues in Testing NISTIR
Haines, J., Zissman, M. Intrusion Detection Systems

While intrusion detection systems are becoming ubiquitous defenses in today's networks, currently we have no comprehensive and scientifically rigorous methodology to test the effectiveness of these systems. This paper explores the types of performance measurements that are desired and that have been used in the past. We review many past evaluations that have been designed to assess these metrics. We also discuss the hurdles that have blocked successful measurements in this area and present suggestions for research directed toward improving our measurement capabilities.

Micheals, R.J., Grother, P., Phillips, The NIST Human ID Evaluation NISTIR 6983 and AVBPA 2003
P.J. Framework

The NIST HumanID Evaluation Framework, or HEF, is an effort to design, implement, and deploy standards for the robust and complete documentation of the biometric system evaluation process. The HEF is an attempt to leverage contemporary technologies, specifically XML, for the formal description of such tests. The HEF was used to facilitate the administration of the 2002 Face Recognition Vendor Test, or FRVT 2002. Unlike FRVT 2000 or FERET 96, FRVT 2002 used both still and video facial imagery, warranting the development of a more sophisticated and regular means of describing data presented to the participants.

Miller, L.E. Joint Distribution of Link Distances 2003 Conference on Information
Sciences and Systems, The Johns
Hopkins University, March 12-14, 2003

The calculation of two-hop connectivity between two terminals for randomly deployed wireless networks requires the joint probability distribution of the distances between these terminals and the terminal that is acting as a relay. In general the distances are not independent since a common terminal is involved. The marginal distributions for link distances are known for various random deployment models. However, the joint distribution of two or more link distances is not known. In this paper, the derivation of the joint distribution is given in general form and in a new form suitable for computation for a network of terminals randomly deployed in a square area.

Miller, L.E., Song, N., Kwak, B. On the Stability of Exponential Backoff NIST Journal of Research

New analytical results are given for the stability and performance of the exponential backoff (EB) algorithm. Previous studies on the stability of the (binary) EB have produced contradictory results instead of a consensus: some proved instability, others

showed stability under certain conditions. In these studies, simplified and/or modified models of the backoff algorithm were used to make analysis more tractable. In this paper, care is taken to use a model that reflects the actual behavior of backoff algorithms. We show that EB is stable under a throughput definition of stability; the throughput of the network converges to a non-zero constant as the offered load N goes to infinity. We also obtain the analytical expressions for the saturation throughput for a given number of nodes, N . The analysis considers the general case of EB with backoff factor r , where BEB is the special case with $r = 2$. We show that $r = 1/(1 - e^{-1})$ is the optimum backoff factor that maximizes the throughput. The accuracy of the analysis is checked against simulation results.

Okun, V., Black, P.E., Yesha, Y. Testing with Model Checkers: Insuring Fault Visibility NISTIR 6929 and 2002 WSEAS International Conference on Applied Mathematics and Computer Science (AMCOS '02) Rio de Janeiro, Brazil

To detect a fault in software, a test case execution must be chosen so intermediate errors propagate to the output. We describe two modeling methods for specification-based mutation testing using model checkers that guarantee this propagation. We evaluate the methods empirically and show that they yield more useful tests than the previous "direct reflection" methods.

Patel, J.K., Kim, S-U., Su, D.H. Modeling Attack Problems and Protection Schemes for All-Optical Transport Networks Accepted for Optical Networks Magazine, SPIE

In All-Optical Transport Networks (AOTN), fault survivability issues are quite similar to those encountered in electro-optic networks that regenerate signals at the network node. On the other hand, attack survivability issues concerning physical fiber security in AOTNs require a new approach taking into consideration the AOTNs physical characteristics. Furthermore, attack detection and isolation schemes may no longer have access to the overhead bits that are otherwise used in legacy networks to transport supervisory information between repeaters or switching sites to perform their functions. This paper presents an analysis of attack and protection problems in AOTNs and proposes a conceptual framework for modeling attack problems and protection schemes for AOTNs.

Patel, J.K., Kim, S-U., Su, D.H. QoS Recovery Schemes Based on Differentiated MPLS Services in All-Optical Transport Next Generation Accepted for International Journal of Photonic Network Communications, Kluwer Academic

The Internet is evolving from best-effort service toward an integrated or differentiated service framework with Quality-of-Service (QoS) assurances that are required for new multimedia service applications. Given this increasing demand for high bandwidth Internet with QoS assurances in the coming years, an IP/MPLS-based control plane combined with a wavelength-routed Dense Wavelength Division Multiplexing (DWDM) optical network is seen as a very promising approach for the realization of future re-configurable transport networks. Fault and attack survivability issues concerning physical security in a DWDM All-Optical Transport Network (AOTN) require a new approach taking into consideration AOTN physical characteristics. Furthermore, unlike in electronic networks that regenerate signals at every node, attack detection and isolation schemes may not have access to the overhead bits used to transport supervisory information between regenerators or switching sites to

perform their functions. This paper presents an analysis of attack and protection problems in an AOTN. Considering this, we propose a framework for QoS guarantees based on the Differentiated MPLS Service (DMS) model and QoS recovery schemes against QoS degradation caused by devices failures or attack-induced faults in an AOTN. We also suggest how to integrate our attack management model into the NIST's simulator Modeling, Evaluation and Research of Lightwave Networks (MERLiN).

Phillips, J.P., Grother, P., Micheals, R., Blackburn, D.M., Tabassi, E., Bone, J.M.	Face Recognition Vendor Test 2002: Evaluation Report	NISTIR 6965 (http://www.itl.nist.gov/iad/894.03/face/face.html#FRVT2002)
---	--	--

The Face Recognition Vendor Test (FRVT) 2002 is an independently administered technology evaluation of mature face recognition systems. FRVT 2002 provides performance measures for assessing the capability of face recognition systems to meet requirement for large-scale real world applications. Ten commercial firms participated in FRVT 2002. FRVT 2002 computed performance statistics on an extremely large dataset—121,589 operational facial images of 37,437 individuals. FRVT 2002 1) characterized identification and watch list performance as a function of database size, 2) estimated the variability in performance for different groups of people, 3) characterized performance as a function of elapsed time between enrolled and new images of a person and 4) investigated the effect of demographics on performance. FRVT 2002 shows that recognition from indoor images has made substantial progress since FRVT 2000. Demographic results show that males are easier to recognize than females and that older people are easier to recognize than younger people. FRVT 2002 also assessed the impact of three new techniques for improving face recognition: three-dimensional morphable models, normalization of similarity scores, and face recognition from video sequences. Results show that three-dimensional morphable models and normalization increase performance, and that face recognition from video sequences offers only a limited increase in performance over still images. For FRVT 2002, a new XML-based evaluation protocol was developed. This protocol is flexible and supports evaluations of biometrics in general.

Podio, F.L., Dunn, J.S., Reinert, L., Tilton, C.J., O'Gorman, L., Collier, P., Jerde, M., Wirtz, B.	Common Biometric Exchange File Format (CBEFF), Augmented	NISTIR 6529-A
---	--	---------------

This report is an augmentation of the original standard, which was published as NISTIR 6529 (January 2001). Common Biometric Exchange File Format (CBEFF) describes a set of data elements necessary to support biometric technologies in a common way. These data can be placed in a single file used to exchange biometric information between different system components or between systems. The result promotes interoperability of biometric-based application programs and systems developed by different vendors by allowing biometric data interchange. CBEFF's initial conceptual definition was achieved through a series of three Workshops co-sponsored by the National Institute of Standards and Technology and the Biometric Consortium. A Technical Development Team, formed as a result of these Workshops, developed CBEFF, as described in this publication, in coordination with industrial organizations (i.e., the BioAPI Consortium, the X9.F4 Working Group, the International Biometric Industry Association, and the Interfaces Group of TeleTrust), and end users. CBEFF provides forward compatibility accommodating for technology improvements and allows for new formats to be created. CBEFF implementations simplify integration of software and hardware provided by different vendors. Further development (e.g., a CBEFF's smart card format) is proposed under the umbrella of the recently formed Biometrics Interoperability, Performance, and Assurance Working Group co-sponsored by NIST and the Biometric Consortium.

Przybocki, M.A., Martin, A.F.

NIST's Assessment of Text
Independent Speaker Recognition

COST 275 Workshop "The Advent
of Biometrics on the Internet"

NIST has coordinated annual evaluations of text-independent speaker recognition since 1996. These evaluations aim to provide important contributions to the direction of research efforts and the calibration of technical capabilities. They are intended to be of interest to all researchers working on the general problem of text-independent speaker recognition. The evaluations have focused primarily on speaker detection in the context of conversational telephone speech. The evaluations are designed to foster research progress with the objectives of exploring promising new ideas in speaker recognition, developing advanced technology incorporating these ideas, and measuring the performance of this technology. Evaluation participants have included commercial, academic and governmental research laboratories from around the world. This paper reviews how NIST assesses speaker recognition systems through our series of benchmark evaluations, focusing on the 2002 NIST Speaker Recognition evaluation.

Radack, S., Editor

Security of Public Web Servers

ITL Bulletin, December 2002

This ITL Bulletin summarizes NIST Special Publication 800-44, Guidelines on Securing Public Web Servers.

Radack, S., Editor

Security for Telecommuting and
Broadband Communications

ITL Bulletin, November 2002

This bulletin summarizes NIST SP 800-46, Security for Telecommuting and Broadband Communications, published September 2002. The report discusses both technical and policy issues, and provides guidance on using personal firewalls, strengthening the security of personal computers and web browsers, protecting home networks, and using virtual private networks.

Radack, S., Editor

Secure Interconnections for Information
Technology Systems

ITL Bulletin, February 2003

This bulletin summarizes NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems, which provides guidance for planning, establishing, maintaining, and terminating secure yet cost-effective interconnections between IT systems that are owned and operated by different organizations.

Radack, S., Editor

Security for Wireless Networks and
Devices

ITL Bulletin, March 2003

This ITL Bulletin summarizes NIST Special Publication 800-48, Wireless Network Security, 802.11, Bluetooth, and Handheld Devices.

Radack, S., Editor

Security of Electronic Mail

ITL Bulletin, January 2003

This ITL Bulletin summarizes NIST Special Publication (SP) 800-45, Guidelines on Electronic Mail Security, September 2002, which helps federal agencies improve the secure design, implementation, and operation of their electronic mail servers and clients.

Roberts, J.W.

Temporal Capture and Sequence
Reconstruction for Evaluation of

SPIE Electronic Imaging '03
Conference

two sets: one whose members appear linearly in the model and another whose members appear nonlinearly. The variable projection algorithm iterates only on the nonlinear parameters and computes the estimates of the linear parameters by a linear least squares calculation. This provides a great advantage for the user, not only because the iteration is simpler, but also because initial estimates are required only for the nonlinear parameters. These advantages are illustrated by applying the method to models for measured time series records of annual global total fossil fuel emissions of carbon dioxide and annual global average temperatures.

Sanders, G.A., Le, A.N.

Effects of Speech Recognition
Accuracy on Performance of DARPA
Communicator Spoken Dialogue

International Journal of Speech
Technology (ISSN 1381-2416)

The DARPA Communicator program explored ways to construct better spoken-dialogue systems, with which users interact via speech alone to perform relatively complex tasks such as travel planning. During 2000 and 2001 two large data sets were collected from sessions in which paid users did travel planning using the Communicator systems that had been built by eight research groups. The research groups improved their systems intensively during the ten months between the two data collections. In this paper, we analyze those data sets to estimate the effects of speech recognition accuracy, as measured by Word Error Rate (WER), on other metrics. We found correlation between WER and Task Completion. That correlation, unexpectedly, remained more or less linear even for high values of WER. The picture for User Satisfaction metrics is more complex: we found little effect of WER on User Satisfaction for WER less than about 35% to 40% in the 2001 data. The size of the effect of WER on Task Completion was less in 2001 than in 2000, and we believe this difference is due to improved strategies for accomplishing tasks despite speech recognition errors, which is an important accomplishment of the research groups who built the Communicator implementations. We show that additional factors must account for much of the variability in task success, and we present multivariate linear regression models for task success on the 2001 data. We also discuss the apparent gaps in the coverage of metrics for spoken dialogue systems.

Schmitz, T.L., Burns, T.J.

Receptance Coupling for High-Speed
Machining Dynamics Prediction

Proceedings of IMAC-XXI: A
Conference and Exposition on
Structural Dynamics, Paper 19,
Kissimmee, Florida, February 3-6,
2003

We apply receptance coupling techniques to predict the tool-point frequency response for high-speed machining applications. Building on early work of Duncan, Bishop and Johnson, and more recent work of Ewins, et al., we develop an analytic expression for the frequency response at the free end of the milling cutter from: 1) an analytic model of the tool; 2) an experimental measurement of the holder/spindle sub-assembly; and 3) a set of empirical connection parameters. These parameters are extracted from a single measurement of the tool/holder/spindle assembly at a known tool overhang length using nonlinear least squares estimation. The assembly model can then be used to predict changes in the tool-point receptance for setup variations, such as tool length. The resulting tool-point frequency response is used to calculate the associated stability lobe diagram, which defines regions of stable and unstable cutting zones as a function of chip width and spindle speed and is used to select appropriate machining parameters. A description of the receptance coupling method, as well as a discussion of the system model and selected connection parameters, are provided. Extensive experimental results are also presented.

Scholtz, J.C. Evaluation of Intelligent Information Access Systems American Association of Artificial Intelligence (AAAI) Conference, Acapulco, Mexico, August 9-15, 2003

This paper discusses traditional evaluations for information access systems and proposes metrics more suited for evaluation of intelligent information access systems.

Scholtz, J.C. Theory and Evaluation of Human Robot Interactions Proceedings of HICSS 36, an IEEE publication

Human-robot interaction (HRI) for mobile robots is still in its infancy. Most user interactions with robots have been limited to tele-operation capabilities where the most common interface provided to the user has been the video feed from the robotic platform and some way of directing the path of the robot. For mobile robots with semi-autonomous capabilities, the user is also provided with a means of setting way points. More importantly, most HRI capabilities have been developed by robotics experts for use by robotics experts. As robots increase in capabilities and are able to perform more tasks in an autonomous manner we need to think about the interactions that humans will have with robots and what software architecture and user interface designs can accommodate the human in-the-loop. We also need to design systems that can be used by domain experts but not robotics experts. This paper outlines a theory of human-robot interaction and proposes the interactions and information needed by both humans and robots for the different levels of interaction, including an evaluation methodology based on situational awareness.

Scholtz, J.C., Laskowski, S.J., Morse, E.L., Wichansky, A., Butler, K., Sullivan, K. The Common Industry Format: A Way for Vendors and Customers to Talk About Software Usability Proceedings of the 10th Annual Human-Computer Interaction Conference

One way to encourage software developers to integrate usability engineering into their development process is for purchasers to require evidence of product usability. Until recently this presented a difficulty because usability and "user friendly software" were vague, ambiguous terms. When large corporations purchase software, they use a number of quantitative measurements in their procurement decision-making process, such as the amount of memory needed, results from standard benchmark tests, performance measures, and measures of robustness. This paper describes our efforts to provide a standard method of quantifying usability and reporting on usability testing to include it in procurement decision-making.

Sims, J.S., Hagstrom, S.A. Erratum: Analytic Value of the Atomic Three-Electron Functions [Phys. Rev. A 44,5492(1991)] Physical Review A44, 5492 (1991), Physical Review A

Reference is made to the paper by Remiddi [Phys. Rev. A 44,5492(1991)] where misprints occur in two important equations. We correct the misprints and provide further verification of the correctness of the modified Equations with a short table comparing 30 significant digit results using Remiddi's formula (with the above corrections) and the output of our recently developed triangle integral package.

Smeaton, A.F., Over, P. The TREC-2002 Video Track Report Included in NIST SP 500-251, The Eleventh Text Retrieval Conference (TREC 2002)

TREC-2002 saw the second running of the Video Track, the goal of which was to promote progress in content-based retrieval from digital video via open, metrics-based evaluation. The track used 73.3 hours of publicly available digital video (in MPEG-1/VCD format) downloaded by the participants directly from the Internet Archive (Prelinger Archives) and some from the Open Video Project. The material comprised advertising, educational, industrial, and amateur films produced between the 1930's and the 1970's by corporations, nonprofit organizations, trade associations, community and interest groups, educational institutions, and individuals. 17 teams representing 5 companies and 12 universities --- 4 from Asia, 9 from Europe, and 4 from the US --- participated in one or more of three tasks in the 2001 video track: shot boundary determination, feature extraction, and search (manual or interactive). Results were scored by NIST using manually created truth data for shot boundary determination and manual assessment of feature extraction and search results. This paper is an introduction to, and an overview of, the track framework --- the tasks, data, and measures --- the approaches taken by the participating groups, the results, and issues regarding the evaluation. For detailed information about the approaches and results, the reader should see the various site reports in the final workshop proceedings.

Smeller, J.M., Leigh, S.D.

Potassium Bromate Assay by Redox
Titrimetry Using Arsenic Trioxide

NIST Journal of Research, Vol.
108, No. 1, pp. 49-55,
January-February 2003

Bromate, a disinfectant, is one of the analytes of interest in wastewater analysis. Environmental laboratories have a regulatory need for their measurements to be traceable to NIST standards. Bromate is not currently certified as a NIST Standard Reference Material (SRM). A traceable assay of potassium bromate (KBrO_3) is needed. KBrO_3 was dissolved in water and assayed by redox titrimetry using arsenic trioxide (As_2O_3). A nominal (0.1 g) sample of As_2O_3 was dissolved in 10 mL of 5 mol/L sodium hydroxide. The solution was acidified with hydrochloric acid, and about 95 % of the KBrO_3 titrant was added gravimetrically. The end point was determined by addition of dilute (1:3) titrant using an automated titrator. The KBrO_3 assay was determined to be 99.76 % \pm 0.20 %. The estimated uncertainty considered the titrations of three independently prepared KBrO_3 solutions.

Snelick, R.D., Indovina, M., Yen,
J., Mink, A.

Multimodal Biometrics: Issues in Design
and Testing

Proceedings of the Fifth
International Conference on
Multimodal Interfaces (ICMI'03),
Vancouver, B.C., Canada,
November 5-7, 2003

The results of experimental studies on multimodal biometric systems for small-scale populations have shown better performance compared to single-mode biometric systems. We examine if such techniques scale to larger populations, introduce a methodology to test the performance of such systems, and assess the feasibility of using commercial off-the-shelf (COTS) products to construct deployable multimodal biometric systems. A key aspect of our approach is to leverage confidence level scores from preexisting single-mode data. An example of a multimodal biometrics system analysis is presented that explores various normalization and fusion techniques for face and fingerprint classifiers. This multimodal analysis uses a population of about 1000 subjects, which is a population size ten-times larger than used in any previously reported study. Experimental results combining face and fingerprint biometric classifiers reveal significant performance improvement over single-mode systems.

Song, D. Post-Measurement Nonlocal Gates Physical Review A

Several proposed quantum computer models include measurement processes, in order to implement nonlocal gates and create necessary entanglement resources during the computation. We introduce a scheme in which the measurements can be delayed for two- and three-qubit nonlocal gates. We also discuss implementing arbitrary nonlocal gates when measurements are included during the process.

Souppaya, M., Harris, A.,
McLarnon, M., Selimis, N. Systems Administration Guidance for
Securing Microsoft Windows 2000
Professional System NIST SP 800-43
([http://csrc.nist.gov/publications/
nistpubs/index.html](http://csrc.nist.gov/publications/nistpubs/index.html))

The document is intended to assist the users and system administrators of Windows 2000 Professional systems in configuring their hosts by providing configuration templates and security checklists. The guide provides detailed information about the security features of Win2K Pro, security configuration guidelines for popular applications, and security configuration guidelines for the Win2K Pro operating system. The guide documents the methods that the system administrators can use to implement each security setting recommended. The principal goal of the document is to recommend and explain tested, secure settings for Win2K Pro workstations with the objective of simplifying the administrative burden of improving the security of Win2K Pro systems. This guidance document also includes recommendations for testing and configuring common Windows applications. The application types include electronic mail (e-mail) clients, Web browsers, productivity applications, and antivirus scanners. This list is not intended to be a complete list of applications to install on Windows 2000 Professional, nor does it imply NIST's endorsement of particular commercial off-the-shelf (COTS) products. Many of the configuration recommendations for the tested Windows applications focus on deterring viruses, worms, Trojan horses, and other types of malicious code. The guide presents recommendations to protect the Windows 2000 Professional system from malicious code when the tested applications are being used.

Splett, J.D., Wang, C.M. Uncertainty in Reference Values for
the Charpy V-notch Verification Journal of Testing and Evaluation

We present a method for computing the combined standard uncertainty for reference values used in the Charpy machine verification program administered by the National Institute of Standards and Technology. The technique is compliant with the ISO GUM and models the between-machine bias using a Type B distribution. We demonstrate the method using actual data from the Charpy machine verification program.

Stanford, V.M., Garofolo, J.S.,
Galibert, O.P., Michel, M., Laprun,
C.D. The NIST Smart Space and Meeting
Room Projects: Signals, Acquisition,
Annotation, and Metrics Proceedings of the 2003 IEEE
International Conference on
Acoustics Speech and Signal

Pervasive Computing devices, sensors, and networks, provide infrastructure for context aware smart meeting rooms that sense ongoing human activities and respond to them. This requires advances in areas including networking, distributed computing, sensor data acquisition, signal processing, speech recognition, human identification, and natural language processing. Open interoperability and metrology standards for the sensor and recognition technologies can aid R&D programs in making these advances. The NIST Smart Space and Meeting Room projects are developing tools for data formats, transport, distributed

processing, and metadata. We are using them to create annotated multi modal research corpora and measurement algorithms for smart meeting rooms, which we are making available to the research and development community.

Stanford, V.M., Kasianowicz, J.J.	Using HMMs to Quantify Signals from DNA Driven Through a Nanometer Scale Pore	2002 Genomic Signal Processing Conference website (http://www.gensips.gatech.edu)
-----------------------------------	---	---

It was recently shown that individual molecules of single-stranded DNA can be forced through a nanoscale pore by an electric field. We demonstrate signal processing methods to detect and measure sub-states in the DNA-induced current blockades during transport. The current flow is approximately piecewise stationary during these transport events, and we used an ergodic HMM to make maximum likelihood estimates of the event sub-states. Interestingly, the signal amplitude distributions caused by polynucleotides with the same length and composition depends on the direction the polymers transit the pore. Our methods indicate automatic extraction of structural information from individual DNA molecules is possible.

Stoneburner, G.R.	COTS Security Protection Profile – Operating Systems (CSPP-OS) (Worked Example Applying Guidance of NISTIR-6462, CSPP) Version 1.0	NISTIR 6985
-------------------	--	-------------

CSPP-OS provides a worked example of the guidance in NISTIR-6462 for the development of Common Criteria Protection Profiles for commercial off the shelf (COTS) information technology. The intended audience consists of those individuals and organizations in both government and private sectors who are tasked with the responsibility to develop or review Protection Profiles. This document is presented as a protection profile, followed by a rationale that is structured as a separate document. This format was selected to facilitate using this guidance as a template for the development of Protection Profiles.

Swanson, M., Bartol, N., Hash, J., Sabato, J., Graffo, L.	Security Metrics Guide for Information Technology Systems	NIST SP 800-55
---	---	----------------

This document provides guidance on how an organization, through the use of metrics, identifies the adequacy of in-place security controls, policies, and procedures. It provides an approach to help management decide where to invest in additional security protection resources or when to research the causes of nonproductive controls. It explains the metric development and implementation process and how it can also be used to adequately justify security control investments. The results of an effective metric program can provide useful data for directing the allocation of information security resources and should simplify the preparation of performance-related reports.

Swanson, M., Fabius, J., Stevens, M., McLarnon, M.	Automated Security Self-Evaluation Tool User Manual, 2003 Edition	NISTIR 6885, 2003 Edition
--	---	---------------------------

The Automated Security Self-Evaluation Tool (ASSET) automates the process of completing a system self-assessment. ASSET will assist organizations in completing the self-assessment questionnaire contained in NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems. This manual is intended to help users of ASSET understand each function of the tool

and how the tool can be used to complete self-assessments. The target audience of this manual is the assessor/manager.

Tebbutt, J.M.	Better Conformance Testing Through Automation: A Software-Based Approach to Creating Conformance Tests for W3C XML Schema	XML Europe 2003 Conference Proceedings
---------------	---	--

This paper describes our experiences in developing a highly configurable, extensible, component-based tool for the creation of conformance tests for XML (eXtensible Markup Language) Schema. It discusses our goals in building the tool; the needs it was designed to fill; its architecture; and finally its capabilities and limitations. The tests produced consist of a set of schemas, each with a corresponding set of instance documents. Alongside the test files themselves is produced a set of metadata, which enables fully automated processing and result presentation of the test collection. The tool achieves this by combining information obtained from the normative Schema for schemas and a local XML control document, using a java class library to generate the required test values, and wrapping these values appropriately. To date, the tool is capable of producing conformance tests for all Schema built-in simple datatypes, including list and union datatypes. Some 6,000+ tests produced by the tool are currently included in the World Wide Web Consortium's test suite for XML Schema. We are also experimenting with incorporating the tool in the automation of test production for XML Query. Our aim as testers is to develop a tool which is flexible, extensible, responsive, easily configurable and modifiable, and which enables us to provide broad coverage of the Recommendation while at the same time minimizing our involvement in individual test production and simplifying the testing procedure for product developers. We believe this tool is a good first step towards that end.

Voorhees, E.M.	The Eleventh Text Retrieval Conference (TREC 2002)	NIST SP 500-251
----------------	--	-----------------

TREC 2002 is the latest in a series of workshops designed to foster research in information retrieval and related tasks. This year's conference consisted of seven different tasks: cross-language retrieval, filtering, interactive retrieval, novelty detection, question answering, content-based access to video, and web-based retrieval. The overview summarizes the conference including the basics of how TREC is organized, summaries of the main results of each of the TREC 2002 tasks, and reports on initial plans for TREC 2003.

Voorhees, E.M.	Evaluating the Evaluation: A Case Study Using the TREC 2002 Question Answering Track	Proceedings of the 2003 Human Language Technology Conference (HLT-NAACL 03)
----------------	--	---

Evaluating competing technologies on a common problem set is a powerful way to improve the state of the art and hasten technology transfer. Yet poorly designed evaluations can waste research effort or even mislead researchers with faulty conclusions. Thus it is important to examine the quality of a new evaluation task to establish its reliability. This paper provides an example of one such assessment by analyzing the task within the TREC 2002 question answering (QA) track. The analysis demonstrates that comparative results from the new task are stable, and empirically estimates the size of the difference required between scores to confidently conclude that two runs are different.

Voorhees, E.M.	Overview of the TREC 2002 Question	Included in NIST SP 500-251, The
----------------	------------------------------------	----------------------------------

The TREC question answering track is an effort to bring the benefits of large-scale evaluation to bear on the question answering problem. The track contained two tasks in TREC 2002, the main task and the list task. Both tasks required that the answer strings returned by the systems consist of nothing more or less than an answer in contrast to the text snippets containing an answer allowed in previous years. A new evaluation measure in the main task, the confidence-weighted score, tested a system's ability to recognize when it has found a correct answer.

Wack, J.P., Tracy, M.

Guideline on Network Security Testing

NIST SP 800-42

The purpose of this document is to provide guidance for security program manager, technical managers, functional managers, and other information technology (IT) staff members who deal with systems concerning when and how to perform tests for network security vulnerabilities and policy implementation. This document identifies network testing requirements and how to prioritize testing activities with limited resources. It describes security testing techniques and tools. This document provides guidance to assist organizations in avoiding redundancy and duplication of effort by providing a consistent approach to network security testing throughout an organization's networks. Furthermore, this document provides a feasible approach for organizations by offering varying levels of network security testing as mandated by an organization's mission and security objectives. The main focus of this document is the basic information about techniques and tools for individuals to begin a testing program. This document is by no means all-inclusive and individuals and organizations should consult the references provided in this document as well as vendor production descriptions and other sources of information.

Wang, C.M., Iyer, H.K.

Uncertainty Calculation for the Ratio of
Dependent Measurements

Metrologia

In this paper we consider the problem of computing an uncertainty interval a ratio with a prescribed confidence level. Although an exact confidence interval procedure, known as the Fieller interval, is available for this problem, practitioners often use various non-exact methods. One such non-exact method is based on the propagation of error approach described in the ISO Guide to the Expression of Uncertainty in Measurement to calculate the standard uncertainty. A confidence interval with presumed confidence level of 95% is obtained by using a coverage factor $k = 2$. We demonstrate that, using $n-1$ degrees of freedom for the standard uncertainty, and the corresponding coverage factor of the t table value, leads to uncertainty intervals which are nearly identical to Fieller's exact intervals whenever the measurement relative uncertainties are small. In addition, they are easy to compute and may be recommended for routine use in metrological applications.

White, D.R.

Update to "Using File Hashes to
Reduce Forensic Analysis"Web (<http://www.nsr.nist.gov>)

This is an update to an article published by another author about NIST Standard Reference Data (SRD) set #28. The quality of the NIST data set was questioned, and this article uses the most recent SRD set in similar experiments, and also in expanded experiments.

Winkel, P., Zhang, N.F.

Serial Correlation of QC Data on the

Clinical Chemistry

Use of Proper Control Charts

Biochemical quality control data have been reported to be autocorrelated. Serial correlation may increase the rate of false alarms and decrease that of true alarms if traditional control charts are used. In this paper, the times series were examined and the performance of the EWMAST chart was compared to that of the EWMA chart in the presence of correlation.

Zhang, N.F.

A Study on the Variance Estimation for
a Stationary Process in SPC

Proceedings of the American
Statistical Association

Recently, statistical process control (SPC) methodologies have been developed to accommodate autocorrelated data. To construct control charts for stationary process data, the process variance needs to be estimated. For an independently identically distributed sequence of a random variable, the variance is usually estimated by the sample variance. For a weakly stationary process, different estimators of the process variance can be used. In this paper, comparisons of estimators of the process variance are made based on the criterion of minimum squared error.